(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－110558

(43)公開日　平成５年(1993)４月30日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		9194－5L		
			7117－5K	Ｈ０４Ｌ　9/00	Ｚ

審査請求　未請求　請求項の数１(全　９　頁)

(21)出願番号　特願平3－270982

(22)出願日　平成３年(1991)10月18日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　田代　成
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝映像メディア技術研究所内

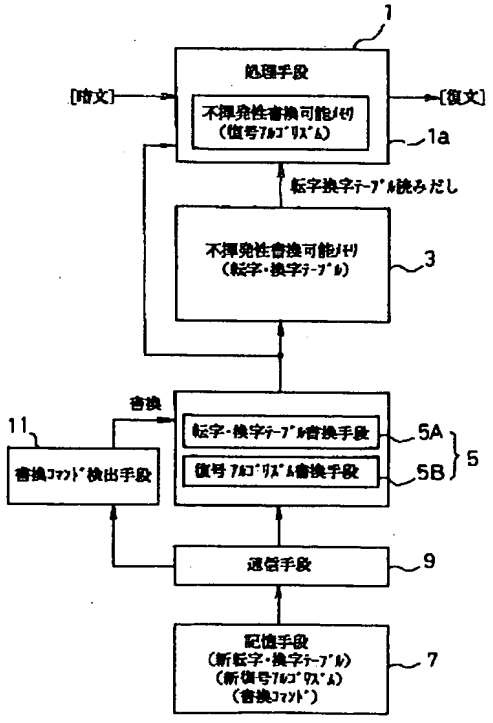
(74)代理人　弁理士　三好　秀和　(外４名)

(54)【発明の名称】　暗号処理装置

(57)【要約】

【目的】　本発明は、暗号が解読された際に暗号・復号アルゴリズム、転字・換字テーブルの一部もしくは全部を変更する手段を具備する暗号処理装置提供することを目的とする。

【構成】　本発明の暗号処理装置は、平文を暗号化して暗文とし或いは暗号化された暗文を復文化する処理手段１の一部若しくは全部を構成するプログラムの一部若しくは全部を、ＥＥＰＲＯＭ３に格納するようにしている。また、暗号が解読されたような場合には、書換手段５は外部から通信手段９を介して入力される信号によってＥＥＰＲＯＭ３に格納される処理手段１の一部若しくは全部を書き換えて、当該暗号の解読に対処する。



1

【特許請求の範囲】

【請求項１】　平文を暗号化して暗文とし、若しくは暗号化された暗文を復文化する処理手段と、

この処理手段の一部若しくは全部を構成するプログラムの一部若しくは全部を格納する書き換え可能でかつ不揮発性の記憶手段と、

外部から入力される信号によって前記記憶手段に格納される処理手段の一部若しくは全部を書き換える書換手段とを有することを特徴とする暗号処理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、例えば有料放送等で使用される暗号処理装置に関する。

【０００２】

【従来の技術】従来、有料放送等においては平文を暗号アルゴリズムに沿って暗号化し、この暗号化によって得られる暗文が送信され、また受信の際にはこの暗文を復号アルゴリズムに沿って復号化して、各種情報を得るようにしていた。

【０００３】以下、図５を参照して従来の暗号処理装置で使用される暗号・復号アルゴリズムについて説明する。この従来の暗号処理装置で、例えば暗文を復合化する際には処理手段１０１のＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に格納される暗号・復号アルゴリズムに沿って、ＲＯＭ１０３に格納される転字・換字テーブルを読み出し、この転字・換字テーブルを参照して、暗号の復号化を行なうようにしていた。従って、この転字・換字テーブルを変更することが出来れば異なる暗号アルゴリズムとすることができる。

【０００４】一方、この暗号化処理のほとんどが予め設定されたプログラムに従って行われることから、これら暗号・復号アルゴリズム及び転字・換字テーブルは読み出しだけで書き換えの出来ないＲＯＭ上におかれるのが通常である。

【０００５】

【発明が解決しようとする課題】しかしながら、これら暗号は解読される虞が多分に在り、ＲＯＭ上に暗号・復号アルゴリズム及び転字・換字テーブルを設けると、暗号を解読された際に、書き換えが出来ないことから、これら暗号・復号アルゴリズム及び転字・換字テーブルの変更が不可能であり、対処することができない。

【０００６】本発明は上記課題に鑑みてなされたもので、暗号が解読された場合であっても暗号・復号アルゴリズム及び転字・換字テーブルの一部もしくは全部を変更することにより対処し得る暗号処理装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するため本発明は、平文を暗号化して暗文とし、若しくは暗号化された暗文を復文化する処理手段と、この処理手段の一部若しくは全部を構成するプログラムの一部若しくは全部を格納する書き換え可能でかつ不揮発性の記憶手段と、外部から入力される信号によって前記記憶手段に格納される処理手段の一部若しくは全部を書き換える書換手段とを有することを要旨とする。

【０００８】

【作用】本発明の暗号処理装置は、平文を暗号化して暗文とし或いは暗号化された暗文を復文化する処理手段の一部若しくは全部を構成するプログラムの一部若しくは全部を、書き換え可能でかつ不揮発性の記憶手段に格納するようにしている。

【０００９】また、暗号が解読されたような場合には、当該記憶手段が書き換え可能であることから、書換手段は外部から入力される信号によって前記記憶手段に格納される処理手段の一部若しくは全部を書き換えて、当該暗号の解読に対処する。

【００１０】

【実施例】以下、本発明の一実施例を図面に基づいて説明する。図１は本発明が適用されるデコーダの構成を説明するためのブロック図である。この図１に示す第１の実施例においては、暗号及び復号共にほぼ同様であることから、この提案が最も有効に活用される復号の場合を例に説明する。

【００１１】図１において、平文が暗号アルゴリズムに沿って暗号化され、この暗号化によって得られた暗文が送信され、さらに受信された暗文が処理手段１に入力され、この処理手段１で復号アルゴリズムに沿って復号化された復文が出力される状態が示される。この処理手段１は、復号アルゴリズムを格納する不揮発性書換可能メモリ１ａを有しており、この不揮発性書換可能メモリは、例えばＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍａｂｌｅ　ＲＯＭ）が採用される。また、この処理手段１には、転字・換字テーブルを格納する不揮発性書換可能メモリ３が接続される。この不揮発性書換可能メモリ３も処理手段１と同様に、メモリに例えばＥＥＰＲＯＭ等が採用される。

【００１２】この不揮発性書換可能メモリ３には、復号アルゴリズム書換手段５Ｂ及び転字・換字テーブル書換手段５Ａを含む書換手段５が接続されており、この書換手段５は書換コマンド検出手段１１により書換コマンドが検出されたときに処理手段１の復号アルゴリズムと不揮発性書換可能メモリ３の転字・換字テーブルの書換えをそれぞれ行うものである。

【００１３】通信手段９は、デコーダとは別に設けられる、例えば放送局に設備される記憶手段７に記憶される新転字・換字テーブル、新復号アルゴリズム及び書換コマンドを前記書換手段５及び書換コマンド検出手段１１に送出するものであって、通常、無線通信が用いられるが、有線放送等のように有線によるものであっても良く、さらにはデコーダに書換え用として設けられる端子

に直接接続するようなものであっても良い。

【００１４】次に、本実施例における動作を暗文の復文化処理に従って説明する。常態においては、処理手段１に入力された暗文は不揮発性書換可能メモリ１ａに格納される復号アルゴリズムに沿って復号化され復文化されることによって復文化処理が行われる。このとき、復号アルゴリズムは不揮発性書換可能メモリ３に格納される転字・換字テーブルを参照して実行される。

【００１５】また、放送形態の変更若しくは暗号が解読される等して復号アルゴリズム或いは転字・換字テーブルを書換える必要が生じた場合には、有線若しくは無線通信による通信手段９を介して、記憶手段７に記憶される新転字・換字テーブル、新復号アルゴリズム及び書換コマンドがデコーダの書換手段５及び書換コマンド検出手段１１に送信される。この書換コマンドは書換コマンド検出手段１１により検出され、復号アルゴリズム書換手段５Ｂ及び転字・換字テーブル書換手段５Ａに復号アルゴリズム及び転字・換字テーブルの新復号アルゴリズム、新転字・換字テーブルへの書換動作を要求するするものである。

【００１６】従って、書換コマンドが書換コマンド検出手段１１により検出されると、この検出信号が書換手段５に入力され書換え動作が要求され、書換手段５の復号アルゴリズム書換手段５Ｂ及び転字・換字テーブル書換手段５Ａは処理手段１の不揮発性書換可能メモリ１ａに格納される復号アルゴリズム及び不揮発性書換可能メモリ３に格納される転字・換字テーブルがそれぞれ新復号アルゴリズム及び新転字・換字テーブルに書換えられる。

【００１７】上述したように、復号アルゴリズム及び転字・換字テーブルは共に不揮発性書換可能メモリ、たとえばＥＥＰＲＯＭに格納されていることから、復号アルゴリズム書換手段５Ｂ及び転字・換字テーブル書換手段５Ａを含む書換手段５によって行われる書換動作で必要に応じて適宜書き換えが可能である。また、復号アルゴリズム書換手段５Ｂ、及び転字・換字テーブル書換手段５Ａには通信手段９によって記憶手段７に格納される新復号アルゴリズム及び新転字・換字テーブルが与えられることから、必要に応じた迅速な書換えが可能となる。

【００１８】次に図２を参照して第２の実施例について説明する。この第２の実施例においては、暗号及び復号共にほぼ同様であることから、この提案が最も有効に活用される復号処理の場合を例に説明する。尚、図２においては理解のため復号アルゴリズムは書き換えないものとしているが、第１の実施例と同様に行うことによって復号アルゴリズムの書き換えも可能である。

【００１９】この第２の実施例は第１の実施例をさらに発展させたセキュリティの高いシステムであり、暗文を復号アルゴリズムに沿って復合化して復文を出力する処理手段２１と、第１の転字・換字テーブルを格納する第

１の不揮発性書換可能メモリ２３Ａと第２の転字・換字テーブルを格納する第２の不揮発性書換可能メモリ２３Ｂと、転字・換字テーブル書換手段２５と、新転字・換字テーブル抽出手段２７と、書換コマンド検出手段３１と、テーブル指定ビット抽出手段３３及び切換えスイッチ３５によって構成される。

【００２０】この第２の実施例においては、不揮発性書換可能メモリ２３Ａ，２３Ｂ内に２種類の転字・換字テーブル、すなわち第１の転字・換字テーブルと第２の転字・換字テーブルとをそれぞれ格納するようにしている。また、通常システムで使用される暗文はパケットの形で入力され、このパケットは第１の転字・換字テーブル２３Ａで復号できるように暗号がかけられている。また、各パケットには第１の転字・換字テーブル２３Ａを復号に用いるか、第２の転字・換字テーブル２３Ｂを復号に用いるかを選択するテーブル指定ビットが設けられており、このテーブル指定ビットはテーブル指定ビット抽出手段３３によって抽出され、第１の転字・換字テーブルと第２の転字・換字テーブルのどちらの転字・換字テーブルを用いるか選択をするためのスイッチ３５を動作させる。その結果、当該パケットにかけられた暗号を解くための転字・換字テーブルデータが処理手段２１の復号アルゴリズムに与えられる。

【００２１】従って、第１の転字・換字テーブル２３Ａで復号できるように暗号をかけているパケットは常時送られていることから、解読される可能性が高いといえる。そこで暗号が解読された場合、暗号アルゴリズムを変更する必要があるため図３に示される転字・換字テーブルを書き換えるためのパケットが暗文として加えられている。

【００２２】この暗号化入力パケットは、アルゴリズム切り替え信号４１、テーブル指定ビット４３、転字・変換字テーブル変更コマンド４５、第１の転字・変換字テーブル変更データ４７及び第２の転字・変換字テーブル変更データ４９によって構成されており、この内、転字・変換字テーブル変更コマンド４５、第１の転字・変換字テーブル変更データ４７及び第２の転字・変換字テーブル変更データ４９は転字・換字テーブルを書き換える場合のみ用いられる第２の転字・換字テーブル２３Ｂで復号を行う暗号がかけてある。

【００２３】従って、通常この第２の転字・換字テーブル２３Ｂで復号を行う暗号を、上記第１の転字・変換字テーブル変更データ４７及び第２の転字・変換字テーブル変更データ４９に基づく新第１の転字・換字テーブル２３Ａａ及び第２の転字・換字テーブル２３Ｂａに書換えられる間に解くことは不可能であることから、解読者は解読の途中で当該書換えが行われたことを知ることが出来ないまま、今回新たに送信された第１の転字・変換字テーブル変更データ４７及び第２の転字・変換字テーブル変更データ４９の内容を知ることはもちろん、先の

第２の転字・換字テーブル２３Ｂで復号を行う暗号と今回の第１の転字・換字テーブル２３Ａで復号を行う暗号とが途中で切替わった複合的な暗号を解読しなければならなくなり、単にこの新第１の転字・換字テーブル２３Ａａで復号を行う暗号の解読を行うより一層の困難を伴うものとなる。

【００２４】図４は、図１に示す第１の実施例若しくは図２に示す第２の実施例を並列に並べた第３の実施例を示すものである。すなわち、この第３の実施例は、図４において、平文を暗号アルゴリズムに沿って暗号化して得られる暗文をアルゴリズム切り替え検出手段６１を介して、第１のアルゴリズム若しくは第２のアルゴリズムに入力し、この暗文を不揮発性書換可能メモリに格納される復号アルゴリズムに沿って復号化し、さらにこの復合化によって得られた復文を切換えスイッチ６７を介して、出力するものである。

【００２５】具体的には、当初は第１のアルゴリズム６３によって暗号文を送っているものとするときに、この第１のアルゴリズム６３が解読されたことが判明した時点で送出される通信路上のアルゴリズム切り替え信号をアルゴリズム切り替え信号検出手段６１において検出し、当該システムを第２のアルゴリズム６５を使用するようにアルゴリズム切り替え信号を変更する。この間に図１に示す第１の実施例若しくは図２に示す第２の実施例のようにアルゴリズム書換コマンドを書き換えるべき暗号アルゴリズムに対して送り、このアルゴリズム（この場合は第１のアルゴリズム６３）を変更する。再び第２のアルゴリズム６５が解読されたことが判明した時点で、再び第２のアルゴリズム６５を使用している間に書換えられた新しい第１のアルゴリズム６３ａを使用するようにアルゴリズム切り替え信号を変更すると良い。

【００２６】本実施例ではこれらの操作を暗号が解読されたことが判明する毎に繰り返す事で当システムを継続的に運用しながら、暗号が解読されたことが判明した時点でハードウェアをなんら変更する事なく高いセキュリティを保った暗号システムを構築する事ができる。

【００２７】

【発明の効果】以上説明したように、本発明によれば、既存の暗号が解読された場合でも新しい暗号に変更することができるため、常にシステムのセキュリティを保持することができる。

【図面の簡単な説明】

【図１】本発明に係る第１の実施例の構成を示すブロック図である。

【図２】本発明に係る第２の実施例の構成を示すブロック図である。

【図３】図２に示す第２の実施例で使用される転字・換字テーブルの構成を示す図である。

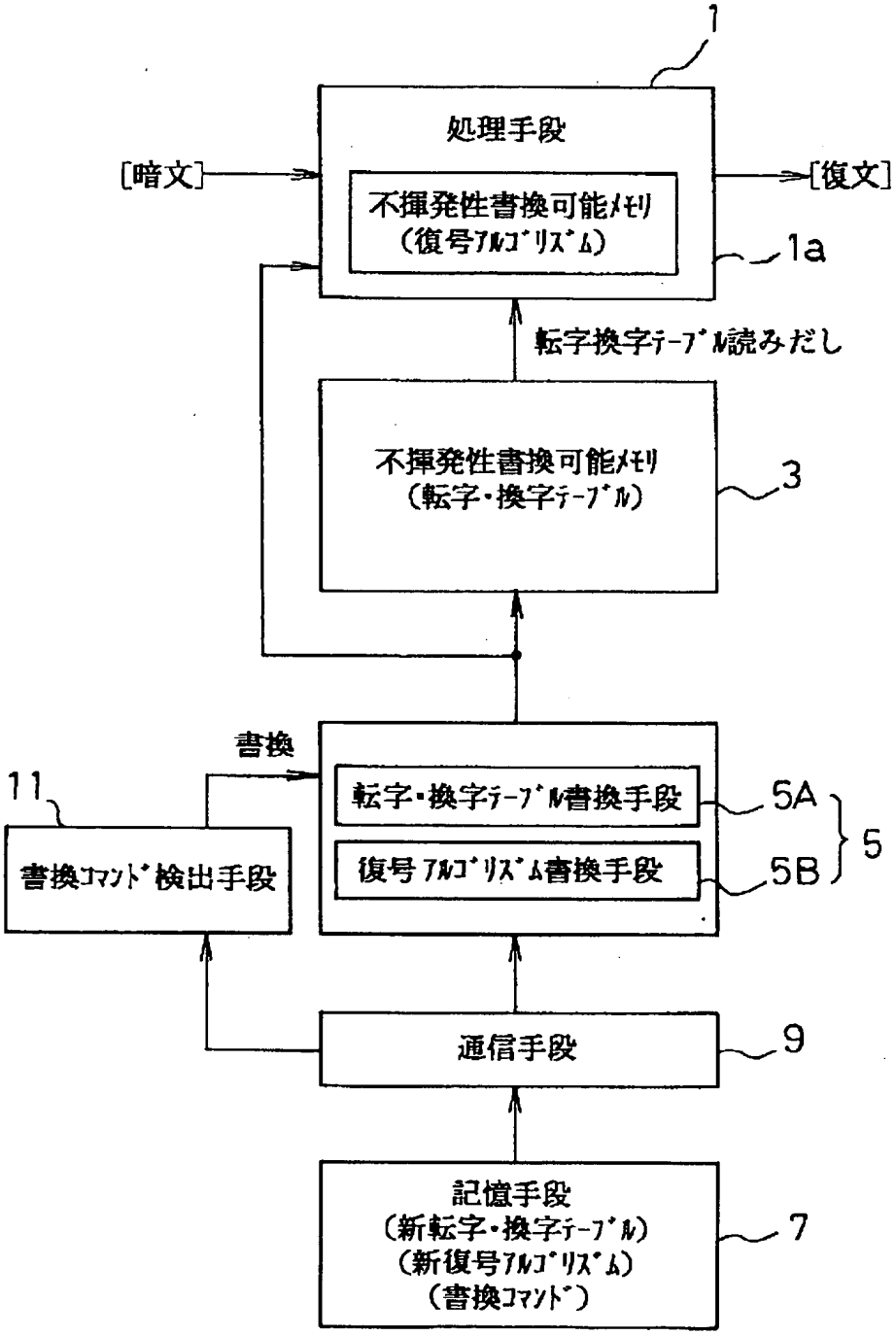
【図４】本発明に係る第３の実施例の構成を示すブロック図である。

【図５】従来の構成を示すブロック図である。

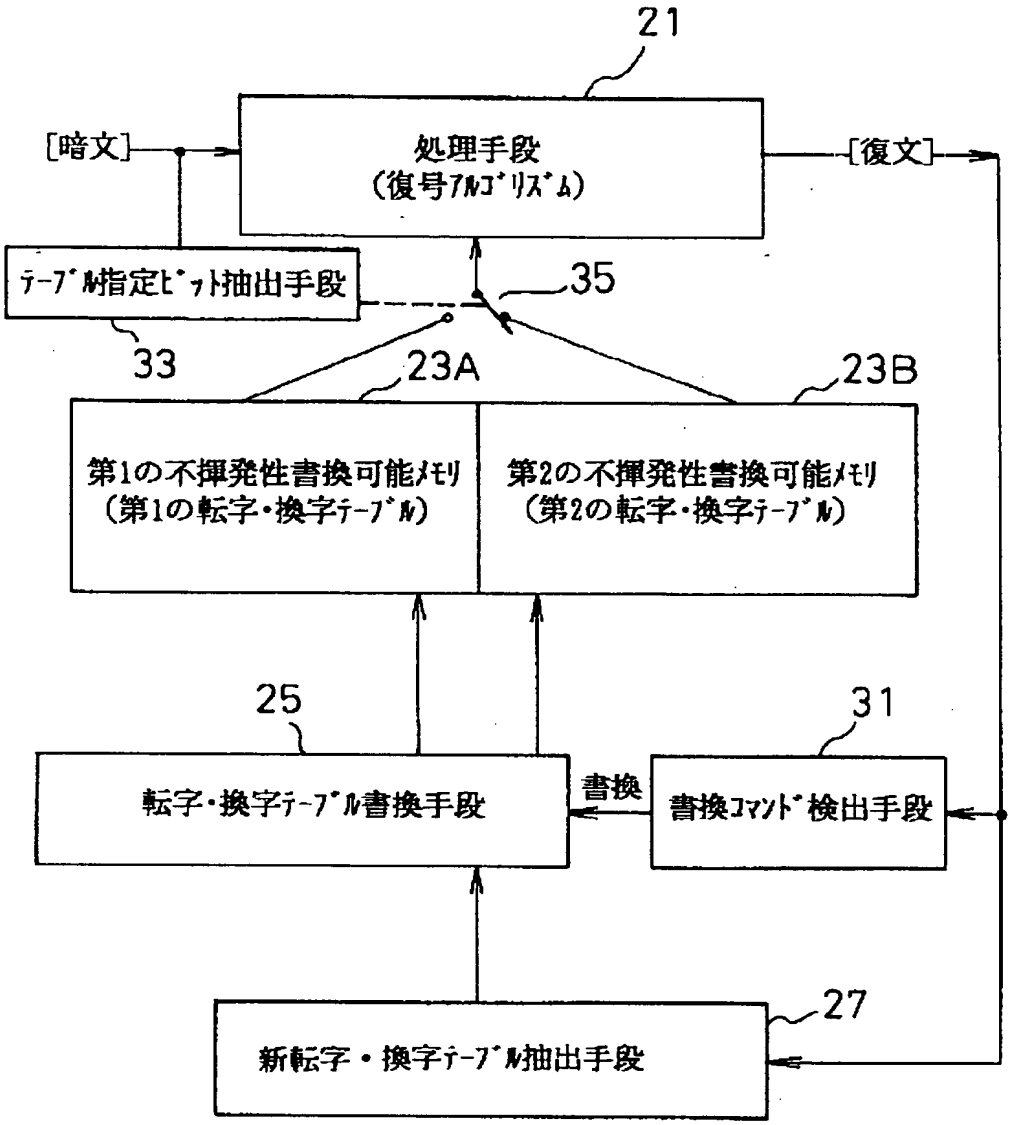
【符号の説明】

１　処理手段
３　不揮発性書換可能メモリ
５Ａ　転字・換字テーブル書換手段
５Ｂ　復号アルゴリズム書換手段
７　記憶手段
９　通信手段
１１　書換コマンド検出手段
２１　処理手段
２３Ａ　第１の不揮発性書換可能メモリ
２３Ｂ　第２の不揮発性書換可能メモリ
２５　転字・換字テーブル書換手段
２７　新転字・換字テーブル抽出手段
３１　書換コマンド検出手段
３３　テーブル指定ビット抽出手段
３５　切換えスイッチ
４１　アルゴリズム切り替え信号
４３　テーブル指定ビット
４５　転字・変換字テーブル変更コマンド
４７　第１の転字・変換字テーブル変更データ
４９　第２の転字・変換字テーブル変更データ
６１　アルゴリズム切り替え検出手段
６３　第１のアルゴリズム
６５　第２のアルゴリズム
６７　切換えスイッチ

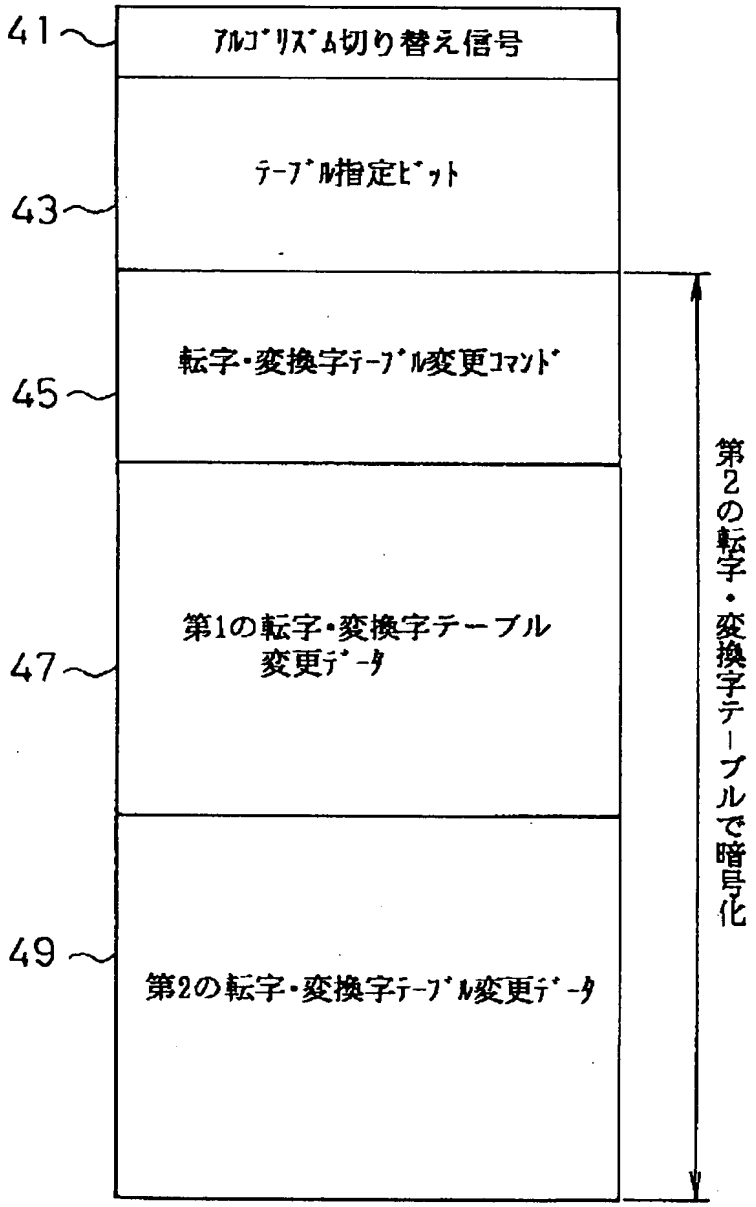
【図１】


1
処理手段
[暗文]
[復文]
不揮発性書換可能ﾒﾓﾘ
(復号ｱﾙｺﾞﾘｽﾞﾑ)
1a
転字換字ﾃｰﾌﾞﾙ読みだし
不揮発性書換可能ﾒﾓﾘ
(転字・換字ﾃｰﾌﾞﾙ)
3
書換
11
転字・換字ﾃｰﾌﾞﾙ書換手段
5A
5
書換ｺﾏﾝﾄﾞ検出手段
復号ｱﾙｺﾞﾘｽﾞﾑ書換手段
5B
通信手段
9
記憶手段
(新転字・換字ﾃｰﾌﾞﾙ)
(新復号ｱﾙｺﾞﾘｽﾞﾑ)
(書換ｺﾏﾝﾄﾞ)
7

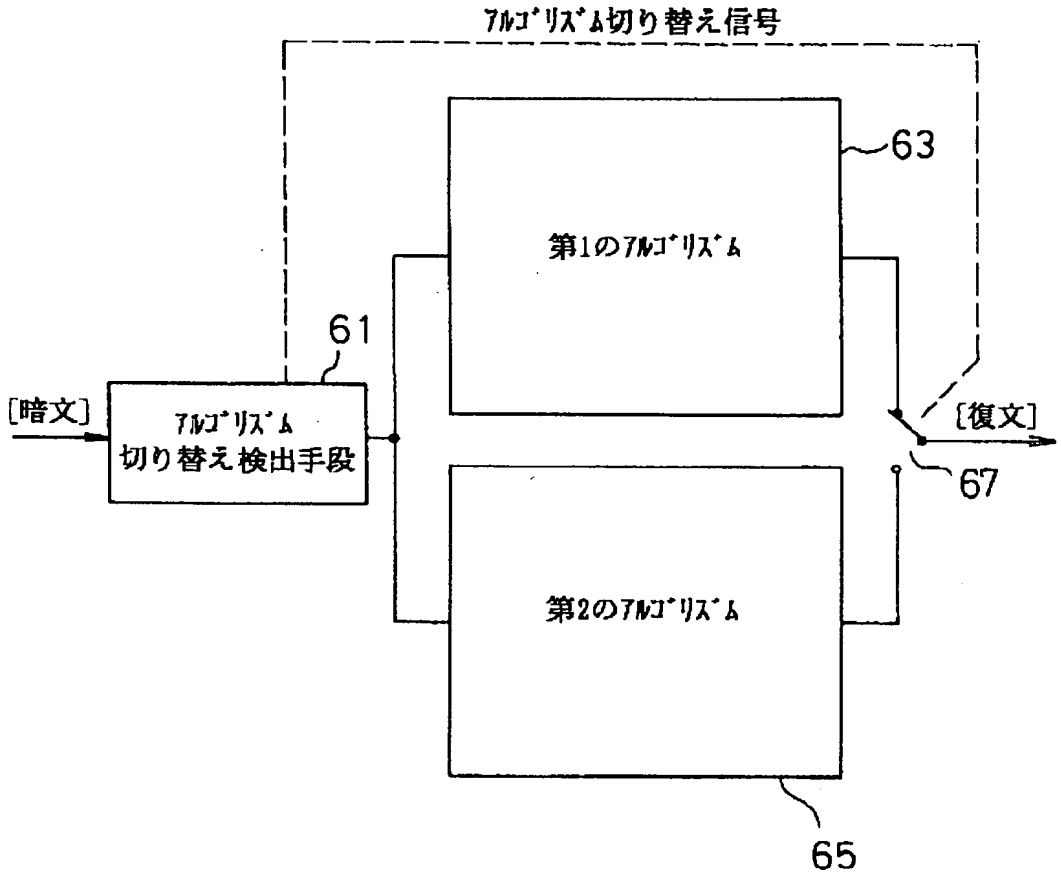
【図2】


21
[暗文]
処理手段
(復号ｱﾙｺﾞﾘｽﾞﾑ)
[復文]
ﾃｰﾌﾞﾙ指定ﾋﾞｯﾄ抽出手段
35
33
23A
23B
第1の不揮発性書換可能ﾒﾓﾘ
(第1の転字・換字ﾃｰﾌﾞﾙ)
第2の不揮発性書換可能ﾒﾓﾘ
(第2の転字・換字ﾃｰﾌﾞﾙ)
25
31
転字・換字ﾃｰﾌﾞﾙ書換手段
書換
書換ｺﾏﾝﾄﾞ検出手段
27
新転字・換字ﾃｰﾌﾞﾙ抽出手段

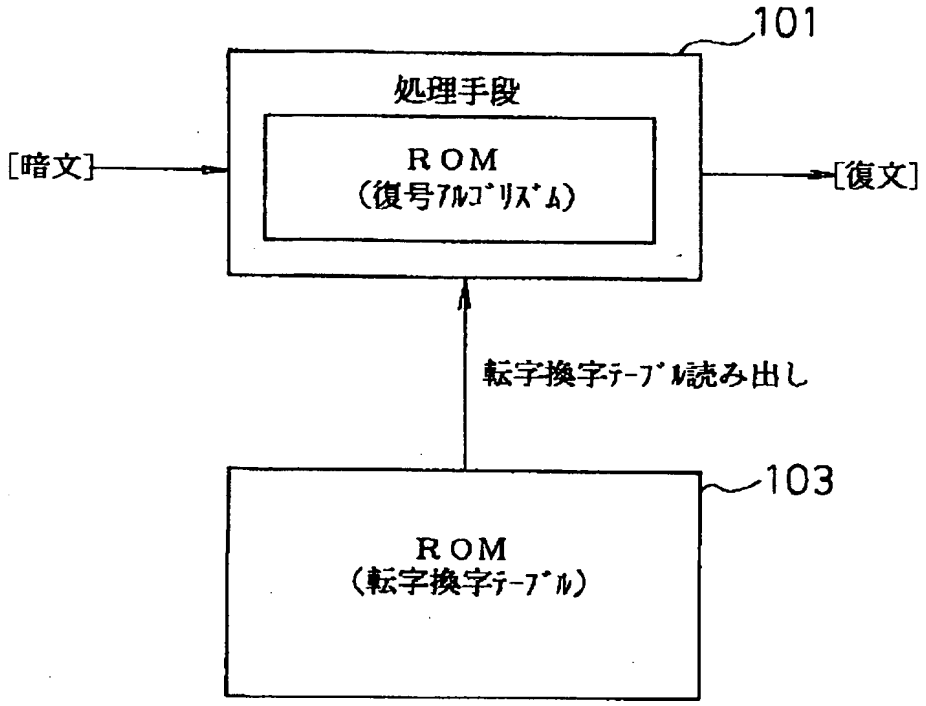
【図３】


41
ｱﾙｺﾞﾘｽﾞﾑ切り替え信号
ﾃｰﾌﾞﾙ指定ﾋﾞｯﾄ
43
転字・変換字ﾃｰﾌﾞﾙ変更ｺﾏﾝﾄﾞ
45
第1の転字・変換字テーブル
変更ﾃﾞｰﾀ
47
第2の転字・変換字ﾃｰﾌﾞﾙ変更ﾃﾞｰﾀ
49
第2の転字・変換字テーブルで暗号化

【図４】


ｱﾙｺﾞﾘｽﾞﾑ切り替え信号
63
第1のｱﾙｺﾞﾘｽﾞﾑ
61
[暗文]
ｱﾙｺﾞﾘｽﾞﾑ
切り替え検出手段
[復文]
67
第2のｱﾙｺﾞﾘｽﾞﾑ
65

【図５】


101
処理手段
ＲＯＭ
（復号ｱﾙｺﾞﾘｽﾞﾑ）
[暗文]
[復文]
転字換字ﾃｰﾌﾞﾙ読み出し
103
ＲＯＭ
（転字換字ﾃｰﾌﾞﾙ）